UEFI on ThinkSystem V3 servers

New features and enhancements

Lenovo

Tool overview

UEFI has the following new features and enhancements for the ThinkSystem V3 platform:

- Version updates to support both Intel and AMD processor ThinkSystem V3 servers
  - UEFI: 2.8
  - PI: 1.7
  - ACPI: 6.4
  - SMBIOS: 3.5.0

New features or enhancements:

- Intel® Optane™ PMem 300 Series new security feature: FIPS (Intel platform only)
- Enhanced Memory RAS features
- SPR-HBM RAS features

The following UEFI features are for AMD-based ThinkSystem V3 servers only:

- AMD Platform Secure Boot (PSB) feature
- AMD Automatic Boot-time Core Disable

PMem 300 Series new security feature: FIPS

- Intel® Optane™ PMem 300 Series (code name: Crow Pass, CPS) is based on a DDR5 interface and supports the Federal Information Processing Standards (FIPS) 140-3 security feature
- The CPS FIPS mode initialization operation is only conducted once, and the FIPS mode initialized state is then maintained until the End of Life (EOL)
- The new CPS from Intel will be in non-FIPS mode by default
- CPS with FIPS mode and non-FIPS mode will have same scope of function
- Mixing Non-FIPS and FIPS CPS DIMMs in one platform is strongly discouraged by Intel
- UEFI can call a CPS FW command to enable FIPS mode – enabling FIPS will totally erase all previous persistent data and the user passphrase

Lenovo CPS FIPS enablement policy

- FIPS mode disabled by default for shipping
- CPS FIPS enablement feature provided on the UEFI setup page, with the following conditions:
  - XCC has the Platinum license (this one-time, opt-in feature cannot be enabled with a trial license)
  - All CPS DIMMs are purchased from Lenovo
- UEFI policy and implementation of FIPS enablement:
  - If a customer enables FIPS mode, UEFI will automatically enable FIPS mode for all CPS DIMMs, including any FRU CPS added in the future
  - If a customer disables FIPS mode, UEFI will not attempt FIPS enablement on that system

UEFI service event logs for CPS issues

UEFI will report the following service event log (SEL) if any CPS DIMM has name space:

- **FQXSFMA0090M** FIPS mode is aborted for PMEM at DIMM [arg1] because it has persistent data region, PMEM identifier is [arg2]

UEFI will report the following SEL if a mix of Non-FIPS and FIPS CPS DIMMs is detected:

- **FQXSFMA0091G** PMEM modules with FIPS mode and non-FIPS mode are mixed in the system.

UEFI will report the following SEL if a customer tries to enable FIPS mode through OneCLI when XCC does not have an adequate license:

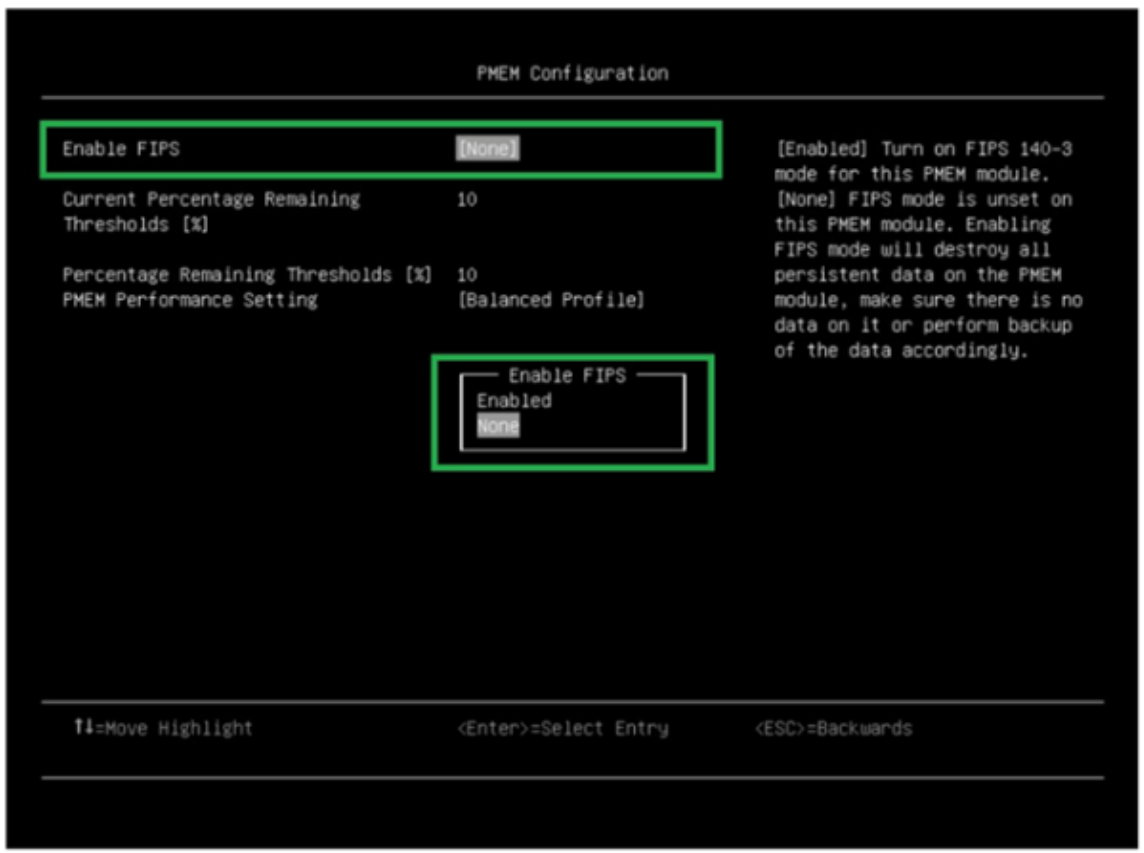
- **FQXSFMA0092M** Cannot enable FIPS mode to the PMEM modules because of inadequate license

UEFI will report the following SEL if FIPS mode cannot be enabled due to CPS FW returning an unexpected status:

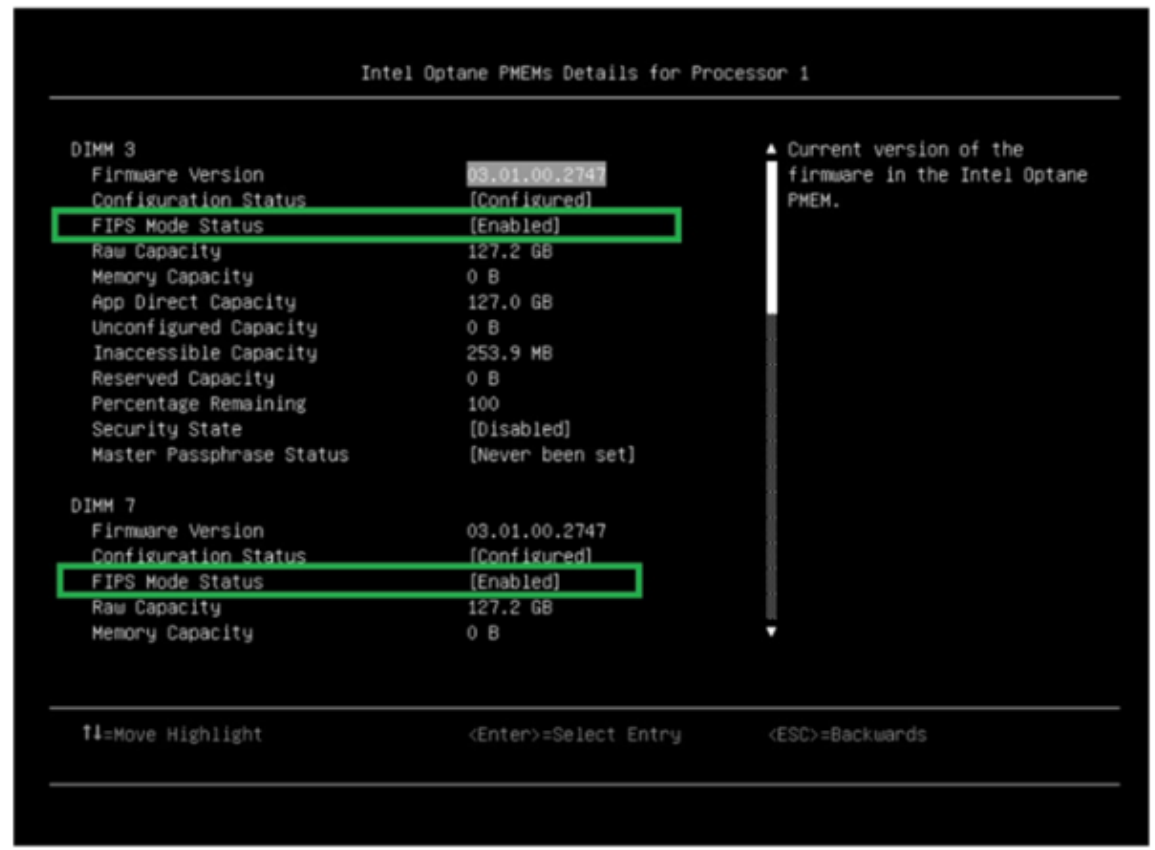
- **FQXSFMA0093M** Failed to enable FIPS mode for PMEM at DIMM [arg1], PMEM identifier is [arg2]

UEFI setup items for CPS FIPS enablement

System settings➔ Intel Optane PMEMs➔ PMEM Configuration



System settings➔ Intel Optane PMEMs➔ Intel Optane PMEMs Details➔ Intel Optane PMEMs Details for Processor #➔ DIMM

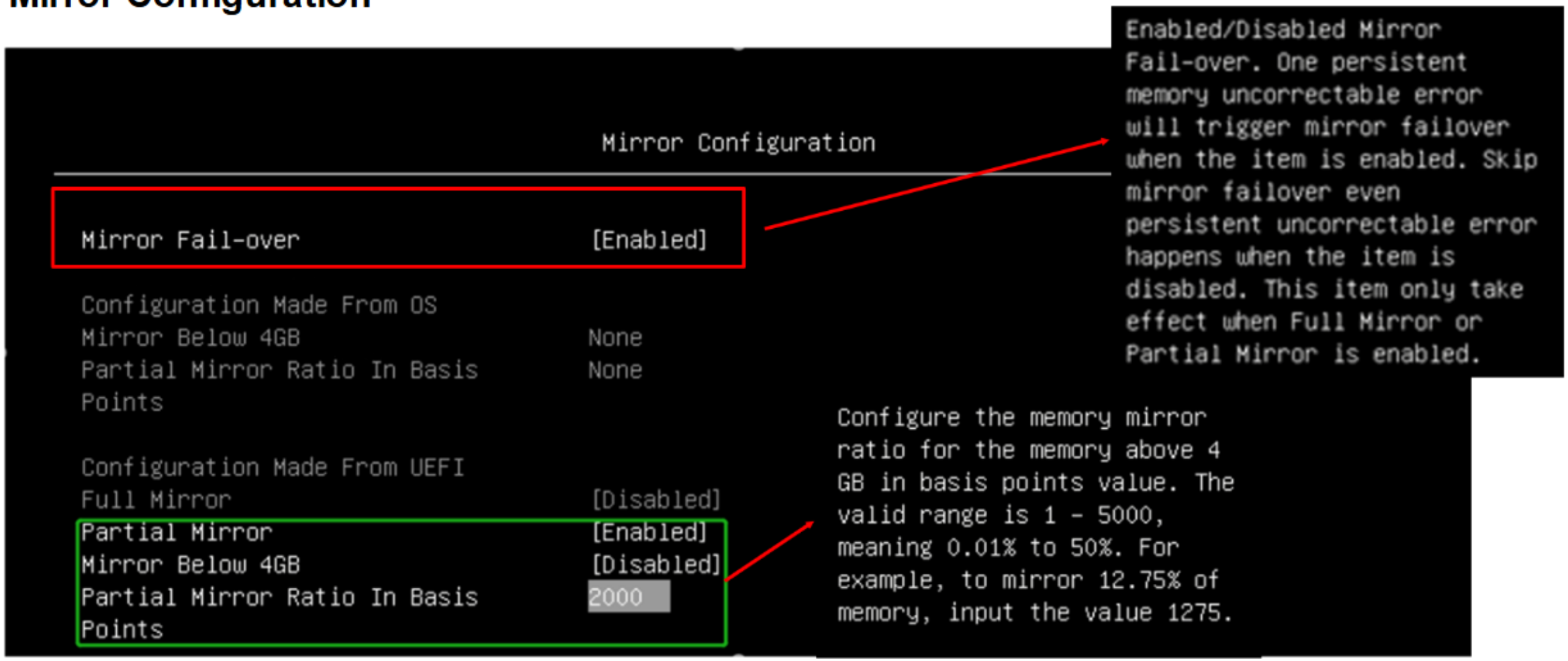


Enhanced memory RAS features – Memory mirroring

- New mirroring fail-over feature support:
  - Enabled: Persistent memory uncorrectable errors trigger mirroring fail-over
  - Disabled: Lenovo value-added, mirroring fail-over is not triggered, but the trigger page is retired to the OS
- Support for full and partial mirroring from both the UEFI setup and the OS
  - Full mirroring is supported by all processors
  - Partial mirroring is supported only by platinum and gold processors
  - Partial mirroring has both a ratio setting and a mirroring below 4 GB setting

Memory mirroring – ThinkSystem UEFI setup page path

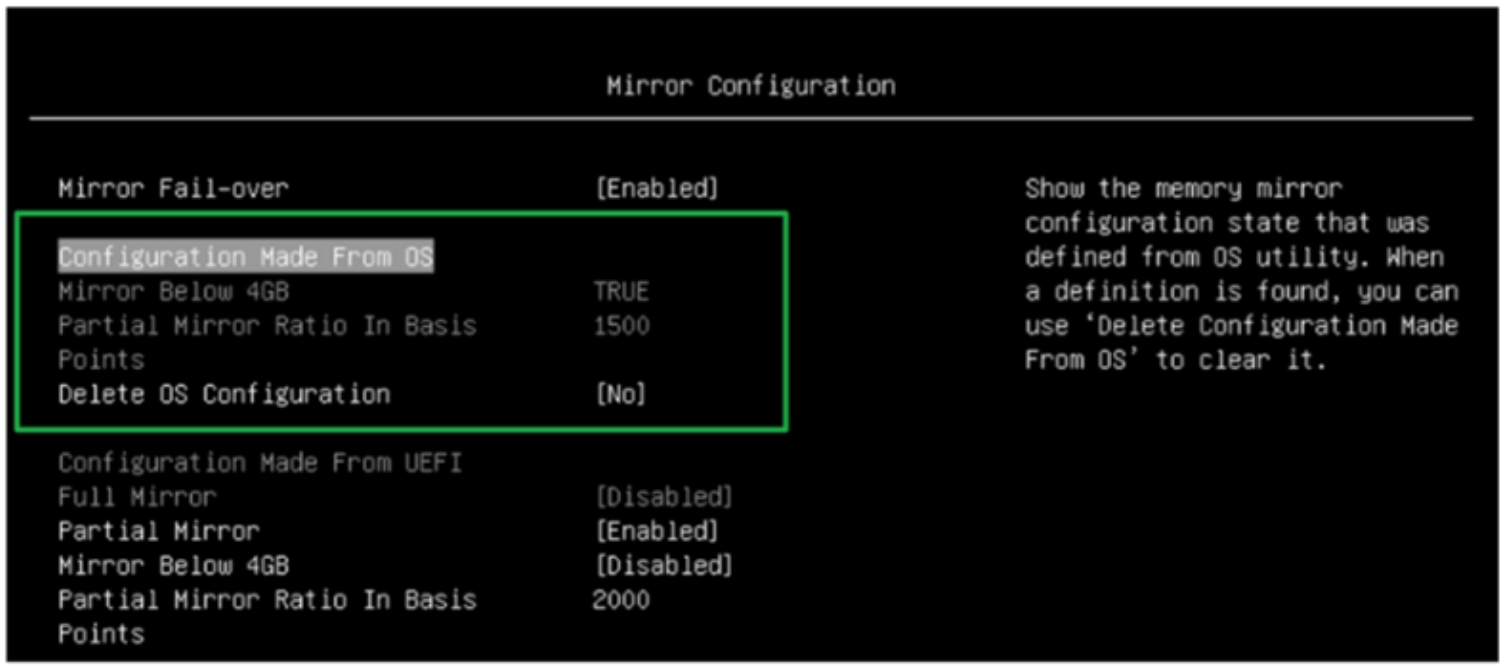
- Go to **System Configuration and Boot Management➔ System Settings➔ Memory➔ Mirror Configuration**



Memory mirroring – configuration from the OS

UEFI will support both UEFI setup page memory mirroring configuration and OS memory mirroring configuration.

- If both configurations exist, the OS mirroring configuration will have the higher priority
- To set or delete the OS mirroring configuration:
  - Set: Use the `efibootmgr` Linux tool to set the configuration from the OS and read only in UEFI
  - Delete: Use `efibootmgr` to set to false/zero for deletion, or use the **Delete** option in UEFI setup



`efibootmgr` command example

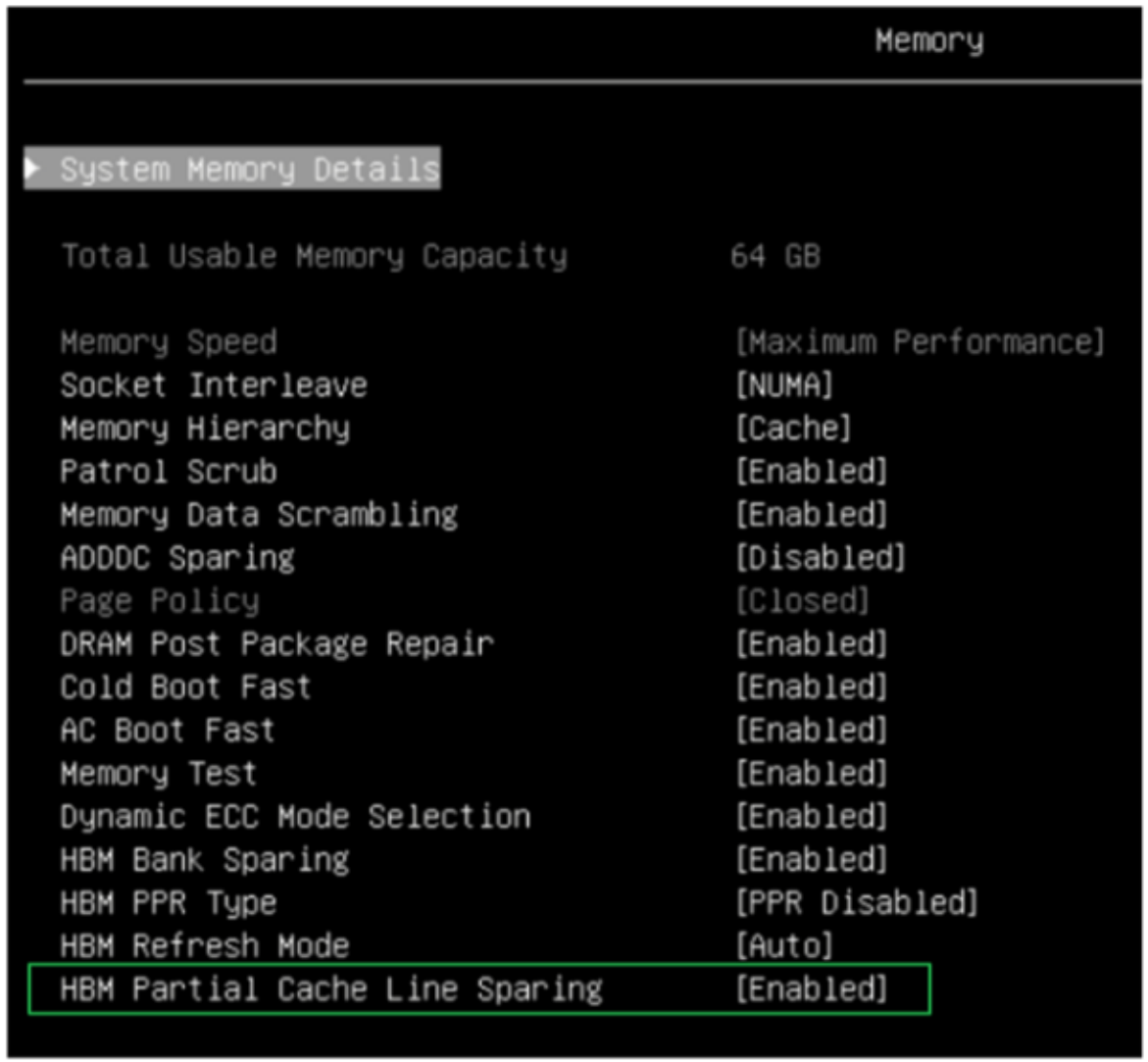
In this example, mirroring below 4 GB and 15% partial mirroring is enabled:

[root@Gold Desktop]# ./efibootmgr -m t -M 15
BootCurrent: 0004
Timeout: 2 seconds
BootOrder: 0004,0003,0002,0000,0001
Boot0000 Enter Setup*
Boot0002 Red Hat Enterprise Linux*
MirroredPercentageAbove4G: 0.00
MirrorMemoryBelow4GB: false
RequestMirroredPercentageAbove4G: 15.00
RequestMirrorMemoryBelow4GB: true

SPR-HBM RAS: Partial cache line sparing

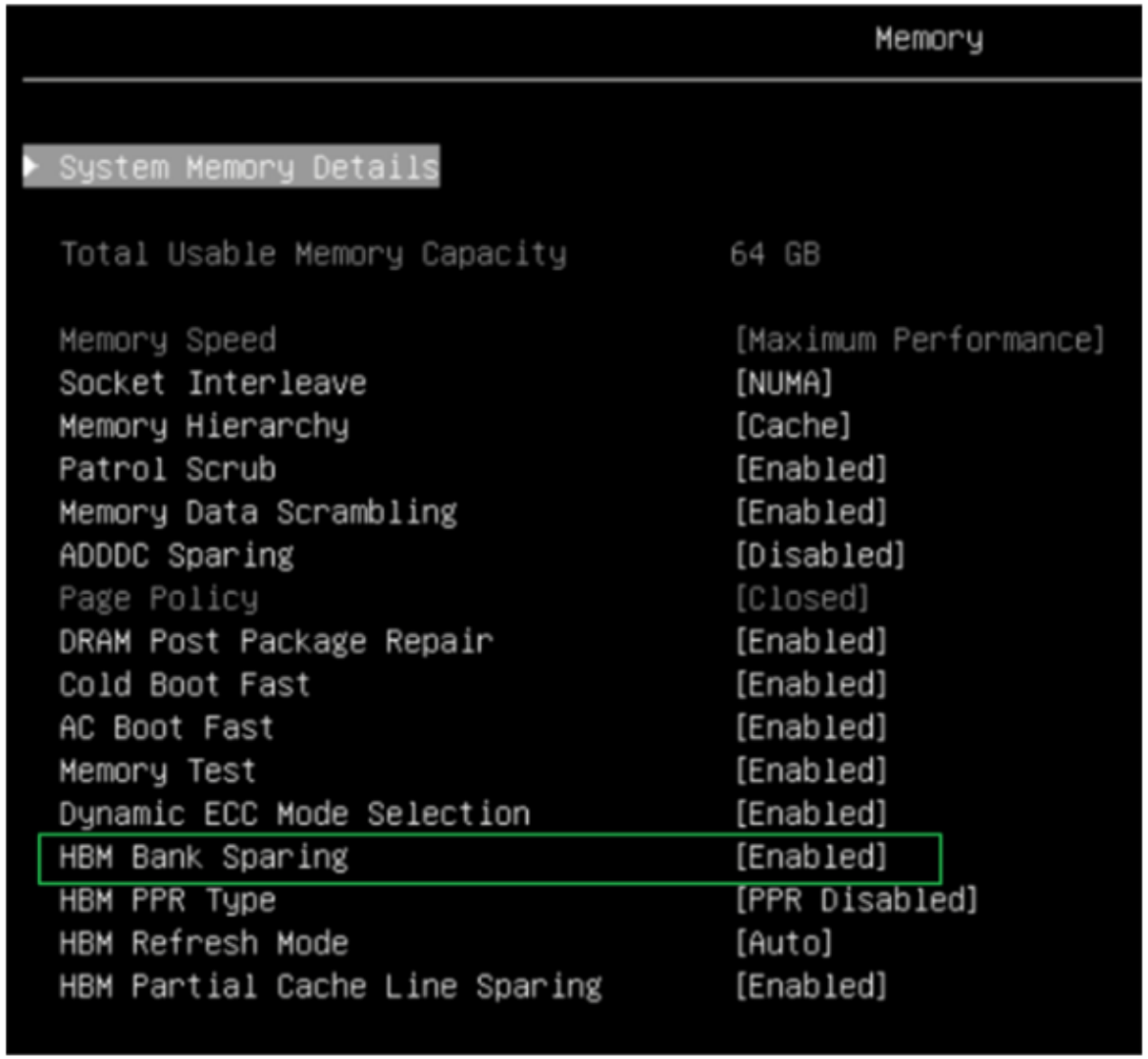
SPR-HBM refers to Sapphire Rapids (SPR) Xeon Scalable processors with high-bandwidth memory (HBM)

- HBM partial cache line sparing (PCLS) design:
  - PCLS is a sparing technique that replaces single DRAM nibble data within a single cache-line size
  - Each HBM pseudo channel has 16 PCLS entries
  - HBM PCLS handling will be triggered if the current error is single bit and persistent
- ThinkSystem UEFI setup item:
  - **System Settings → Memory → HBM Partial Cache Line Sparing** – the default value is **Enabled**.



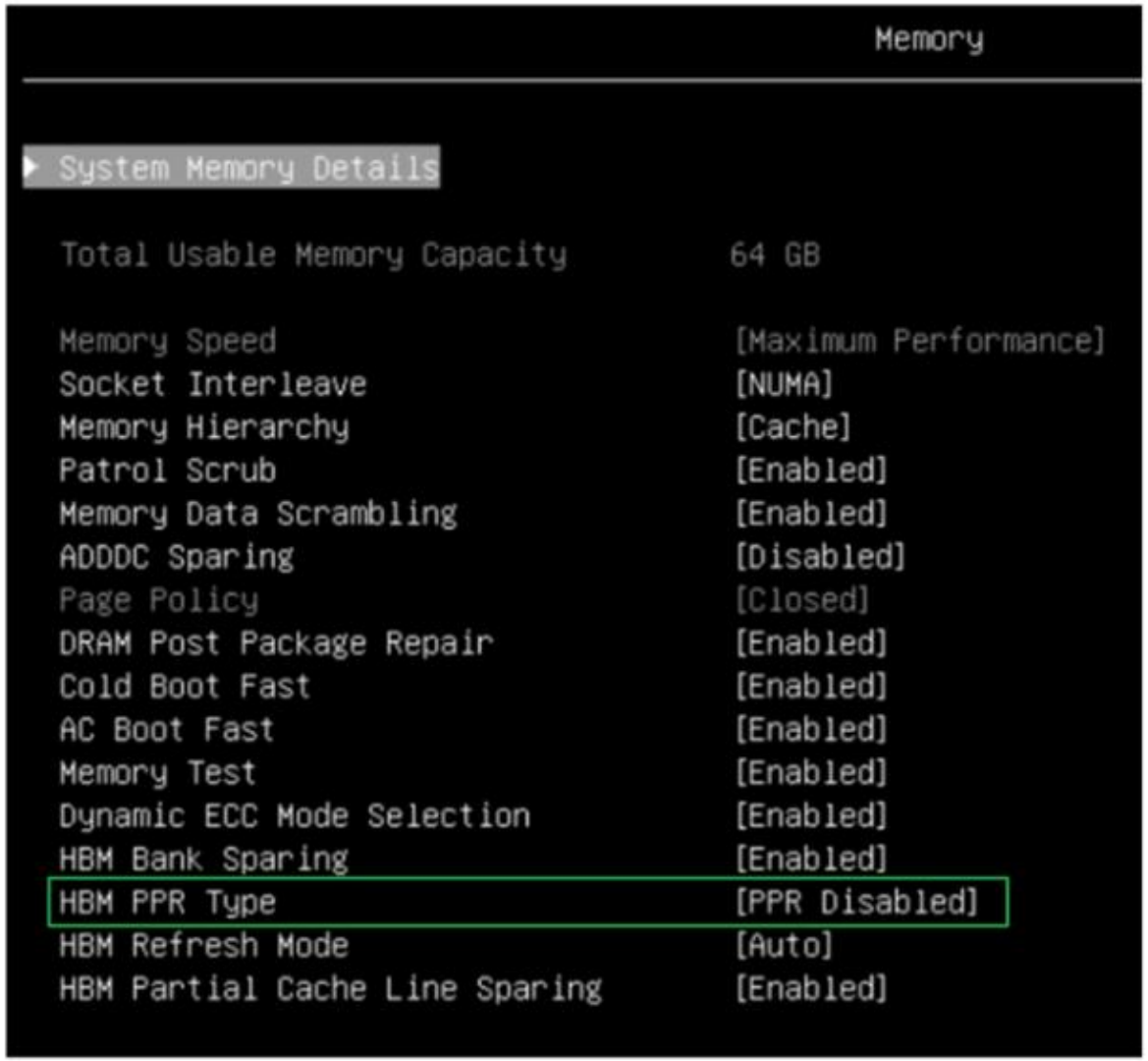
SPR-HBM RAS: Bank sparing

- HBM bank sparing design:
  - 1/16 of the total HBM capacity will be reserved if bank sparing is enabled
  - Enabling bank sparing will result in a loss of 1/16 of HBM capacity
  - Enablement of a SW threshold window (with multi-bit CE), using a bank level thresholder for bank sparing, or PCLS failed/run out of resource
- ThinkSystem UEFI setup item:
  - **System Settings → Memory → HBM Memory Bank Sparing** – the default value is **Disabled**



SPR-HBM RAS: Post package repair

- HBM post package repair design:
  - 20 HBM post package repair (PPR) entries (another 20 DDR5 PPR entries) per system
  - Enablement of a SW threshold window (with multi-bit CE), using a row-level thresholder for PPR requests
  - Single persistent CE to directly trigger a PPR request
  - UE to report PPR
- ThinkSystem UEFI setup item:
  - **System Settings → Memory → HBM PPR Type** – the default value is **Enabled**.



AMD Secure Processor and Platform Secure Boot

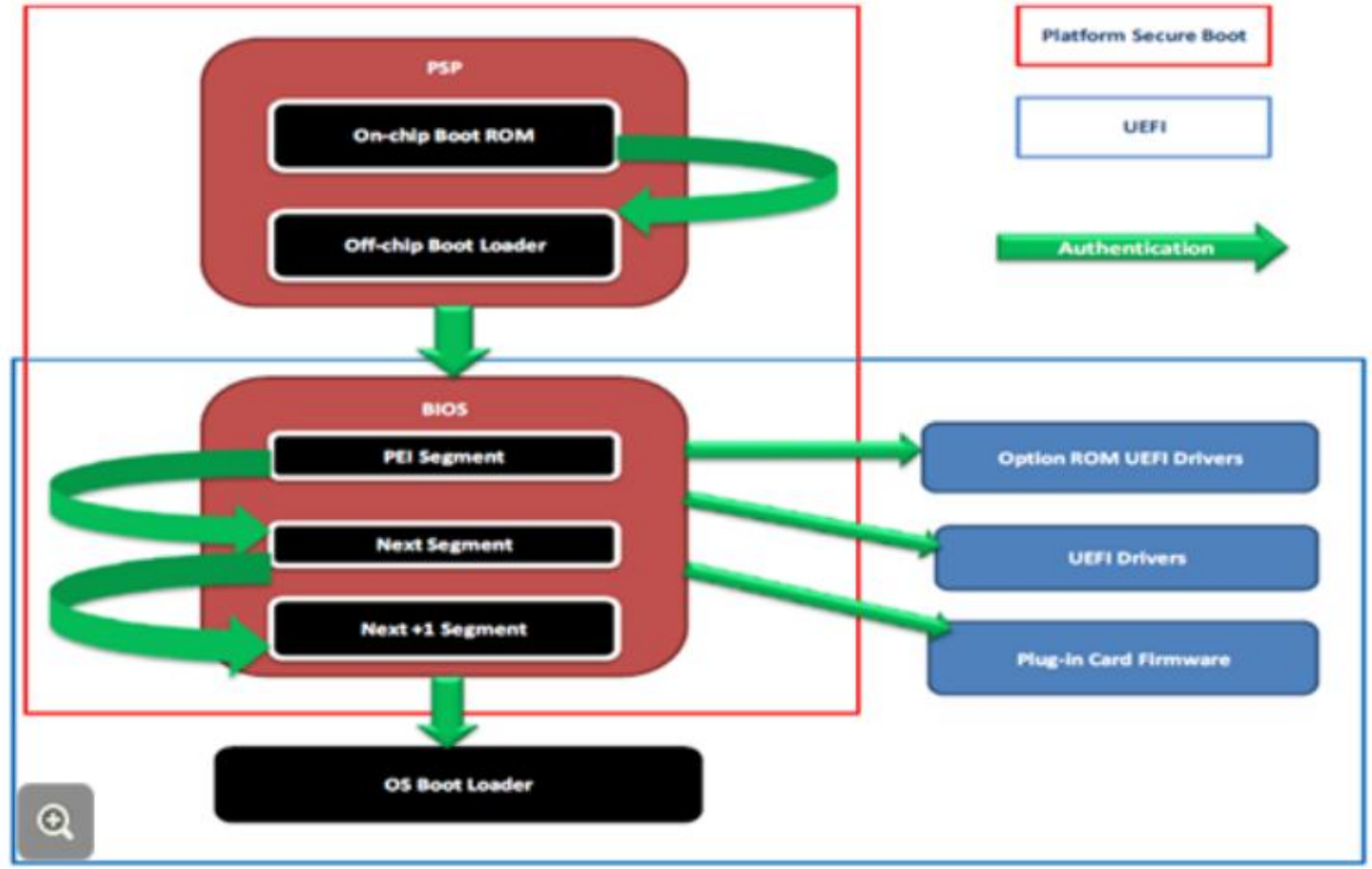
AMD Secure Processor (ASP) and Platform Secure Boot (PSB) is supported by the Lenovo server platform. It is a vendor-locking feature which means you can only move the processor to another Lenovo system board and not to the system board of another vendor – for example, HP or Dell.

AMD processor definition in UEFI

- Neutral CPU – Customer fuse region is not blown: CUSTOMER_KEY_LOCK, PLATFORM_SECURE_BOOT_EN, Vendor ID, and Model ID fuse bits are not set. The CPU is in PSB_NOT_ENABLED state.
- Fused CPU – Customer fuse region is blown: CUSTOMER_KEY_LOCK, PLATFORM_SECURE_BOOT_EN, Vendor ID, and Model ID fuse bits are set. The CPU is in PSB_ENABLED state.

AMD Platform Secure Boot definition

- PSB is intended to assert, via a root of trust (RoT) anchored in the hardware, the integrity and authenticity of a portion of the system ROM image before it can execute.
- In an AMD SoC-based platform, the fixed PSP on-chip boot ROM and the hash of the public part of an AMD root key embedded in it forms this HW root of trust.



Lenovo implementation of PSB fuse

PSB_EOM and PSB_FUSE flags support the PSB fuse operation

- PSB_EOM – Controls the EOM operation; three valid settings can be configured:
  - 0: Non-EOM - Default
  - 1: EOM Enable
  - 2: EOM Done - will be set via UEFI after UEFI completes the PSB fuse operation
- PSB_FUSE – Controls the PSB FUSE operation; two valid settings can be configured:
  - 0: Disable PSB FUSE - UEFI will skip the PSB fuse, leaving it as ECAT default
  - 1: Enable PSB FUSE - UEFI will conduct the PSB fuse in next reboot if EOM is enabled

UEFI will check the value of PSB_EOM and PSB_FUSE

- If PSB_EOM is 1 and PSB_FUSE is 1, UEFI will conduct the fuse operation. Otherwise, UEFI will skip the fuse operation and change the PSB_EOM flag to 2 - EOM done.
  - PSB_ EOM Done can only be set by UEFI, and after PSB_EOM is done, UEFI will ignore the PSB_FUSE flag. When PSB_EOM is done but then XCC resets it to 1, UEFI will execute the EOM process again and change the status to done.
- If the PSB_EOM is 0, UEFI will ignore the PSB_FUSE flag and skip the PSB fuse operation.

Out-of-band configuration commands

Use the following OneCLI commands to configure PSB Fuse:

- Enable PSB FUSE:
  - OneCli.exe config set SYSTEM_PROD_DATA.PSBFUSE "Enable PSB FUSE" -imm IMM_USERID:IMM_PASSWORD@IMM_IP --override
- Disable PSB FUSE:
  - OneCli.exe config set SYSTEM_PROD_DATA.PSBFUSE "Disable PSB FUSE"--imm IMM_USERID:IMM_PASSWORD@IMM_IP --override
- EOM Enable:
  - OneCli.exe config set SYSTEM_PROD_DATA.PSBEOM "EOM Enable" --imm IMM_USERID:IMM_PASSWORD@IMM_IP -override

Field service procedures for CPU replacement

If the service team has to replace a CPU in the field and the customer requests CPU fuse, the servicer needs to execute the following steps:

- Turn off the AC power and replace the CPU.
- Turn on the system and go to the UEFI setup.
- Execute the OOB command to enable PSB fuse.
  - `OneCli.exe config set SYSTEM_PROD_DATA.PSBFUSE "Enable PSB FUSE" –imm IMM_USERID:IMM_PASSWORD@IMM_IP --override`
- Execute the OOB command to enable EOM again.
  - `OneCli.exe config set SYSTEM_PROD_DATA.PSBEOM "EOM Enable" --imm IMM_USERID:IMM_PASSWORD@IMM_IP –override`
- Reboot the system and check the XCC audit log for a new SEL “PSB Fuse Enabled” report
  - This SEL will only report once to identify the current PSB fuse setting. There will be no new SEL reports whenever a PSB fuse operation is complete.
- If there is no new SEL report, call for the next level of support.

For the complete procedures, refer to the following GLOSSE tip page:
How to update PSB fuse state on ThinkSystem AMD v3 machines or the later series

XCC2 PSB audit logs

Event ID	Message	Comment
FQXSFPU4072G	Platform secure boot policy is not defined	UEFI will report “Platform secure boot policy is not defined” on the POST screen, and this event will be reported on the XCC web page before PSB_EOM is set to be enabled
FQXSFPU4070I	Platform secure boot fuse is enabled	UEFI will carry out the PSB fuse operation, and there will be an audit log to identify the current PSB fuse setting (Enable/Disable) after PSB_EOM is set to be enabled
FQXSFPU4071I	Platform secure boot fuse is disabled	

AMD Automatic Boot-time Core Disable feature

The processor has a feature to omit cores from the active configuration if they fail built-in self tests (BIST). If a core or cache fails BIST, the processor will report the core complex(es) in error and attempt to boot using a minimum number of core complexes, subject to population restrictions given in the Processor Programming Reference.
If an error is found, UEFI will send error data to the BMC SEL by reporting a status code, as shown below:

Index	Severity	Source	Common ID	Message
0	⊗	Processors	FQXSFPU0063N	CPU 1 core 24 25 26 27 28 29 30 31 40 41 42 43 44 45 46 47 disabled

UEFI events reference table

Servicers can check UEFI events in the ThinkSystem information center. Search for the system you want to check, and select **UEFI events** to get more information. Use the following link as an example: https://thinksystem.lenovofiles.com/help/index.jsp?topic=%2FSR630V2%2Fuefi_error_messages.html